RAIMONDO ZAGAMI

LA FIRMA DIGITALE TRA SOGGETTI PRIVATI NEL REGOLAMENTO CONCERNENTE « ATTI, DOCUMENTI E CONTRATTI IN FORMA ELETTRONICA »

SOMMARIO: 1. La validità del documento informatico. — 2. Il documento informatico senza firma digitale. — 3. Il documento informatico con firma digitale. — 4. I certificatori. — 5. I certificati. — 6. Firma digitale autenticata. — 7. *Segue*: cybernotary. — 8. Atti pubblici notarili. — 9. Validazione temporale. — 10. Scadenza, revoca e sospensione delle chiavi. — 11. Firma digitale falsa. — 12. Duplicazione, copie, ed estratti del documento. — 13. Trasmissione del documento.

1. LA VALIDITÀ DEL DOCUMENTO INFORMATICO.

L'art. 15[2] della l. 15 marzo 1997, n. 59 è la prima norma che nel nostro ordinamento afferma in termini ampi e generali, sia dal punto di vista oggettivo che soggettivo, il principio della piena validità e rilevanza della documentazione informatica, parificandone il valore a quella cartacea, stabilendo che « gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge ». Dato l'estremo tecnicismo e la rapida evoluzione della materia è, poi, prescritto che « i criteri e le modalità di applicazione del presente comma sono stabiliti [...] con specifici regolamenti da emanare entro centottanta giorni dalla data di entrata in vigore della presente legge ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400 » (regolamenti di delegificazione).

Il primo e più importante regolamento di applicazione, formulato da una commissione istituita in seno all'AIPA (Autorità per l'Informatica nella Pubblica Amministrazione), ispirandosi ampiamente alle soluzioni straniere e sovranazionali[1], è stato appro-

[1] Si segnalano il *Digital Signature Act* dello Utah, la prima legge in materia ad essere approvata il 27 febbraio 1995 (ch. 61-1995), poi modificata nel 1996 (ch. 205-

vato dal Consiglio dei ministri il 31 ottobre 1997[2]. L'art. 2 di tale regolamento ripropone sostanzialmente l'art. 15[2] della l. 59, stabilendo che « il documento informatico da chiunque formato, l'archiviazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge *se conformi alle disposizioni del presente regolamento* ».

Per l'effettivo e concreto riconoscimento del valore giuridico della documentazione informatica e delle firme digitali occorrerà, peraltro, attendere che il regolamento approvato diventi operativo a seguito dell'emanazione degli ulteriori ed indispensabili *regolamenti tecnici* di attuazione, a cui rimanda, in via generale, l'art. 3. Pertanto, non essendo questi ultimi ancora noti, l'analisi del regolamento approvato non può essere che limitata per molti aspetti (non sempre propriamente tecnici) che risultano ancora poco chiari o del tutto da definire e fondata su una serie di ipotesi ed assunti da verificare, considerando anche la sinteticità della relazione di accompagnamento.

2. Il documento informatico senza firma digitale.

Seguendo l'esempio di quasi tutte le legislazioni straniere, il regolamento italiano si apre enunciando le definizioni dei termini tecnici rilevanti per la disciplina giuridica. È subito determinato il concetto di documento informatico in generale, cioè *anche se non sottoscritto con firma digitale*, come « la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti » (art. 1 lett. *a*)[3]. Tale definizione riproduce sostanzialmente, con l'ag-

---

1996); la legislazione della Florida, *Electronic Signature Act*, approvato nel maggio 1996 (SB 0942, ch. 96-224), cui fa seguito *l'Electronic Commerce Act*, del 30 maggio 1997 (HB 1413, ch. 97-241), che prevede il *cybernotary*; la legge tedesca approvata il 13 giugno 1997 (art. 3 della Multimedia Law), ed il relativo progetto di regolamento nell'ultima versione del 7 luglio 1997; ABA, *Digital Signature Guidelines*, 1 agosto 1996, quale schema di riferimento per i legislatori degli Stati Uniti; OCSE, *Guidelines for Cryptographic Policy*, 27 marzo 1997, contenenti una serie di raccomandazioni rivolte agli Stati per indirizzare la loro attività legislativa in materia di cifratura; UNCITRAL, *Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Legal Issues*, February 1997, quale preparazione per una *Model Digital Signature Legislation*, da affiancare alla *Model Law on Electronic Commerce* (May - June 1996); ed, infine, European Commission, ***Ensuring Security and Trust in Electronic Communication - Towards a European Framework for Digital Signatures and Encryption*, 8 ottobre 1997, COM (97) 503, che pone l'obiettivo di armonizzare le differenti legislazioni entro l'anno 2000, allo scopo di assicurare il mutuo riconoscimento delle firme digitali.**

[2] Un primissimo schema è stato presentato nel mese di settembre 1996, anteriormente alla stessa l. 59. Quasi completamente diverso rispetto al primo è lo schema presentato nel mese di giugno del 1997, il quale, con alcune importanti modifiche, è stato poi approvato in via preliminare il 5 agosto 1997; e, quindi, senza modifiche di rilievo, approvato in via definitiva.

[3] L'art. 491-*bis* c.p., introdotto dalla l. 547/1993, definisce il documento informatico come « qualunque supporto informatico contenente dati o informazioni

giunta del termine « informatica », quella che da tempo è stata elaborata dalla dottrina — e che non è mai stata recepita dal legislatore — per individuare il concetto di documento (non ancora informatico)[4].

Seguendo la conclusione di certa dottrina[5], si afferma che il documento informatico munito dei requisiti previsti dal presente regolamento ha l'efficacia probatoria delle *riproduzioni meccaniche* (fotografiche, cinematografiche, fonografiche, ecc.), previste dall'articolo 2712 c.c. (art. 5^2). Pertanto, il documento informatico, *anche senza sottoscrizione digitale*[6], forma piena prova dei fatti e delle cose rappresentate, se colui contro il quale è prodotto non ne disconosce la conformità ai fatti o alle cose medesime[7].

Ancora accogliendo le conclusioni della dottrina, secondo la quale la forma informatica non è altro che un particolare tipo di scrittura[8], si afferma che « il documento informatico *munito dei requisiti previsti dal presente regolamento* soddisfa il requisito legale della forma scritta » (art. 4^1).

3. Il documento informatico con firma digitale.

La firma digitale[9] è definita in relazione alla sua essenza tecnica ed al suo scopo, quale il « il risultato della procedura informatica

aventi efficacia probatoria o programmi specificamente destinati ad elaborarli ».

[4] Sulla nozione di documento vedi F. Carnelutti, ***Documento - teoria moderna***, **in *Nov. dig. it.*, VI, Torino, 1957, p. 85 ss.; C. Angelici, *Documentazione e documento - diritto civile*, in *Enc. giur. Trecc.*, XI, Roma, 1989.**

[5] L. Montesano, ***Sul documento informatico come rappresentazione meccanica nella prova civile*, in *Riv. dir. proc.*, 1987, p. 1 ss.**

[6] L'efficacia probatoria dell'art. 2712 c.c. è assegnata al « documento informatico munito dei requisiti previsti dal presente regolamento » (art. 5^2). Poiché non si fa riferimento ad un documento « sottoscritto con firma digitale », come nel comma precedente, si può ritenere che l'efficacia di riproduzione meccanica sia attribuita al documento informatico *anche se non sottoscritto con firma digitale*. D'altra parte, non avrebbe senso assegnare il valore *ex* 2712 c.c. solo al documento con firma digitale, quando a questo è attribuito già il valore superiore ed assorbente di scrittura privata (art. 5^1). Accogliendo tale interpretazione, per dare un significato all'inciso « munito dei requisiti previsti dal presente regolamento » (art. 5^2), si dovranno attendere le regole tecniche di cui all'art. 3.

[7] Non solo un testo, ma anche un immagine, un suono, un filmato ed in generale qualunque informazione digitalizzabile possono rientrare nella categoria del documento informatico. Così, se da una parte, verrebbe a perdere senso il concetto e la disciplina distinta delle riproduzioni meccaniche previste dall'art. 2712 c.c., dato che viene meno la ragione di distinguere tali mezzi di espressione quanto al loro contenuto, in quanto tutto diventa digitale (vedi R. Zagami, ***Firme « digitali », crittografia e validità del documento elettronico*, in *Dir. inf.*, 1996, p. 170); da un'altra parte, si recupera la loro particolare efficacia probatoria per assegnarla al documento informatico, anche se rappresentante un testo (art. 5^2).**

[8] Vedi R. Borruso, ***Computers e diritto*, 1, Milano, 1988, p. 275 (anche il volume 2, p. 217 e 221); E. Giannantonio, *Manuale di diritto dell'informatica*, Padova, 1997, p. 383 ss.**

[9] La locuzione « firma digitale » è preferibile rispetto ad altre (ad es. « contrasse-

(validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica ed una privata, che consente al sottoscrittore tramite la chiave privata ed al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici » (art. 1 lett. *b*).

Per il regolamento, l'apposizione di una firma digitale è basata *esclusivamente*[10] sull'impiego di sistemi di cifratura detti *asimmetrici*, perché funzionanti con coppie di chiavi collegate (« sistemi di validazione » *ex* art. 1 lett. *c*). Con la *chiave privata*, conosciuta solo dal soggetto titolare e sottoscrittore[11], si firma il documento (art. 1 lett. *e*)[12]; con la corrispondente *chiave pubblica*, destinata

gno elettronico », adottata nello schema di regolamento del 1996; « sigillo informatico », D. Giaquinto e P. RAGOZZO, ***Il sigillo informatico***, **in *Notariato*, 1/1996, p. 80 ss.; « firma » o « sottoscrizione elettronica »), in quanto: si tratta effettivamente di una firma « digitale » (formata da bits), e non « elettronica »; è corrispondente alla locuzione anglofona « digital signature »; non è un semplice « contrassegno », perché la funzione che assolve è proprio quella di una firma; non è una « sottoscrizione », perché nel documento informatico non vi può essere alcuna autografia di un nominativo (« -scrizione »), né tantomeno può essere apposta in calce (« sotto- ») al documento. L'obiezione che la « firma » presuppone un imprescindibile collegamento di tipo personale o somatico è superabile mediante l'impiego dei sistemi di riconoscimento biometrici. Peraltro, il regolamento impiega anche i termini di « sottoscrizione », « sottoscrittore » e di documento « sottoscritto » con firma digitale in diversi articoli (ad es. artt. 1 lett. *b*, 5^1, 10^2, 10^5, 16^2).**

[10] Le « firme digitali » basate sulla criptografia asimmetrica possono essere inquadrate in un concetto più generale di « firma elettronica », che non presuppone necessariamente l'impiego delle tecnologie di cifratura asimmetrica, inteso come qualunque lettera, carattere, o simbolo adottato con l'intento di autenticare uno scritto e *logicamente associato* con questo. Così la legge della Florida (sec. 4), che a queste più generali firme elettroniche riconosce poi l'equivalenza probatoria con la sottoscrizione tradizionale (sec. 5).

[11] Per garantire l'esclusività d'uso delle chiavi private da parte del soggetto titolare, la tecnica preferibile è quella della loro cifratura e dell'incorporazione in *smart cards*, unitamente al controllo mediante sistemi di identificazione *biometrica* (impronte digitali, vocali, della retina, ecc.), definiti dal regolamento come una « sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente » (art. 1 lett. *g*) e da disciplinare ad opera delle emanande regole tecniche (art. 3^3). Sulla diversa funzione svolta dalle firme digitali e dalle firme biometriche e sull'opportunità di usare le seconde per controllare gli accessi alle chiavi private vedi R. ZAGAMI, ***Firme « digitali »*, 1996, cit., p. 166 s. e 168. Una nuova tecnologia denominata PAN (*Personal Area Network*), capace di trasmettere dati informatici grazie alla naturale conduttività elettrica del corpo umano dovuta alla salinità presente nella pelle, utilizzando lievissime correnti elettriche, permetterebbe la trasmissione dei dati informatici occorrenti per le operazioni di apposizione delle firme digitali, mediante il semplice contatto di un dito.**

[12] La firma digitale, tecnicamente, può essere contenuta come appendice allo stesso documento firmato, oppure in un documento separato, senza nulla pregiudicare in ordine alla possibilità di una corretta verifica dell'autenticità. Dal separato documento contenente la firma, occorre però poter risalire al documento principale, dato che il primo, a seguito della decifrazione, restituisce solo un *hash* (art. 10^1, per il quale « a ciascun documento informatico [...] può essere *apposta o associata con separata evidenza informatica*, una firma digitale »).

ad essere divulgata, si verifica la firma digitale già apposta (art. 1 lett. *f*)[13][14].

L'apposizione di una firma digitale, consente di ottenere gli stessi *risultati* della sottoscrizione tradizionale, pur possedendone diversi *requisiti*. È possibile accertare la *provenienza* soggettiva (imputabilità) e *l'integrità* del contenuto di un documento informatico, così come attraverso la tradizionale sottoscrizione e la verifica della consistenza del supporto è possibile accertare, rispettivamente, la provenienza e l'integrità di un documento cartaceo[15]. Pertanto, è stabilito espressamente un generale principio di equivalenza tra la sottoscrizione tradizionale su carta e la *sottoscrizione* con firma digitale (art. 10^2)[16]. Inoltre, la firma digitale sostituisce l'apposizione di « sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere » (artt. 10^7 e 16^3), che ovviamente non potrebbero essere apposti su un documento immateriale.

Conseguenza logica della equivalenza tra i due tipi di sottoscrizioni è l'attribuzione al documento informatico sottoscritto con firma digitale dell'efficacia probatoria della *scrittura pri-*

[13] Alle emanande regole tecniche (art. 1 lett. *o*, art. 3), da adeguare con decorrenza almeno biennale « alle esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche » (art. 3^2), è demandata l'individuazione degli algoritmi da utilizzare, e la determinazione dei requisiti del *software* e *dell'hardware* da impiegare per la generazione di una firma digitale e per la conseguente verifica (il « sistema di validazione » *ex* art. 1 lett. *c*). Nella progettazione e scelta di tali dispositivi si dovrà tener conto che l'apposizione di una firma digitale realizza la *funzione dichiarativa* della sottoscrizione (volontà di assumere la paternità del documento) e dovrebbe poter realizzare la funzione della *ponderatezza* (richiamare l'attenzione delle parti sull'importanza dell'atto che si accingono a compiere). Vedi R. ZAGAMI, ***Firme « digitali »*, 1996, cit., p. 164 s. Occorre quindi che i dispositivi tecnici utilizzati siano tali che una persona può ragionevolmente rendersi conto, in anticipo e senza possibilità di errore, della generazione di una firma digitale e del contenuto dei dati coperti dalla firma; permettano di determinare, in fase di verifica, a quali dati la firma si riferisce, se i dati firmati sono rimasti immodificati (integrità), ed a quale persona la firma è da attribuire (provenienza) (par. 14^2 della legge e par. 16^3 del progetto di regolamento tedesco).**

[14] Mediante l'inversione dell'uso delle chiavi è ottenibile la *cifratura a scopo di segretezza* (art. 1 lett. *d*), fermo restando l'algoritmo utilizzato. La chiave pubblica del destinatario si applica per trasformare il messaggio in un testo incomprensibile ed indecifrabile (art. 1 lett. *f*); l'applicazione della corrispondente chiave privata del destinatario restituisce il testo in chiaro (art. 1 lett. *e*). Il regolamento, in quanto provvedimento riguardante l'autenticazione, pur prevedendo la cifratura a scopo di segretezza, non ne contiene alcuna disciplina, rinviando alle emanande regole tecniche di dettare le misure volte a garantire la riservatezza (confidenzialità) delle informazioni contenute nel documento informatico (art. 3^3). A prescindere dall'eventuale cifratura, il principio della segretezza della corrispondenza trasmessa per via telematica, è ribadito dall'art. 13 ponendo degli obblighi, la cui violazione ricade nella disposizione dell'art. 616 c.p., modificato dalla l. 547/1993 per estenderlo alle comunicazioni telematiche.

[15] Per un confronto tra sottoscrizione tradizionale e firma digitale, con riferimento a requisiti e funzioni di entrambe, vedi R. ZAGAMI, ***Firme « digitali »*, 1996, cit., p. 151 ss.**

[16] Una generale disposizione di equivalenza tra sottoscrizione su carta e firma digitale è presente nella maggior parte delle leggi e progetti stranieri. Ad es. legge della Florida (sec. 5); Utah DSA (sec. 46-3-401); ABA, *Guidelines*, cit., 5.1.

vata ai sensi dell'art. 2702 c.c. (art. 5[1]), senza possibilità di disconoscimento, dato che la sottoscrizione digitale (a seguito di verifica positiva) è già di per sé da considerarsi come « riconosciuta »[17].

4. I CERTIFICATORI.

Il fatto che una chiave pubblica decifri una firma digitale non ha di per sé alcun significato, se non che due chiavi (pubblica e privata) sono matematicamente correlate; mentre, non esiste alcun collegamento intrinseco tra una chiave pubblica ed una persona. È necessario l'intervento di una terza parte fidata ed imparziale, detta *certificatore* (art. 1 lett. *k*)[18], il quale emette i *certificati*, cioè dei documenti digitali attestanti essenzialmente che una certa chiave pubblica è di titolarità di un determinato soggetto (art. 1 lett. *h*).

Con riferimento al settore privato (per la p.a. vige un autonomo sistema *ex* art. 17), per svolgere l'attività di certificatore occorre l'inclusione in un apposito elenco pubblico tenuto dall'AIPA (art. 8^3). I requisiti per l'iscrizione sono in parte mutuati da quelli richiesti per l'esercizio dell'attività bancaria (artt. 14 e 26 d.lgs. 385/1993): *a*) forma di società per azioni[19], con un capitale sociale adeguato (a garanzia del corretto funzionamento del certificatore e dell'adempimento degli eventuali obblighi di risarcimento); *b*) requisiti di onorabilità da parte dei rappresentanti legali e degli amministratori; *c*) affidamento per competenza ed esperienza al fine del rispetto delle norme del regolamento e delle regole tecniche; d) adozione di processi informatici e prodotti conformi a standards internazionali[20]. L'accertamento del possesso dei sud-

[17] Sulla configurabilità di una scrittura privata in forma informatica vedi R. ZAGAMI, ***Firme « digitali »*, 1996, cit., p. 161 s. L'eventuale *accertamento giudiziale* della scrittura privata informatica (artt. 214 ss. c.p.c.) non verterà sulla provenienza (immediatamente riscontrabile) ma, in quanto implicante un controllo sulla legalità, sarebbe solo funzionale all'ottenimento di un titolo per le modifiche dei registri immobiliari (art. 2657 c.c.) e delle imprese (art. 2189 c.c.), similmente all'autenticazione *ex* art. 16.**

[18] Si parla anche, indifferentemente, di Autorità di Certificazione (AC) o *Certification Authority* e di *Trusted Third Party* (TTP). In realtà le AC si distinguerebbero dalle TTP perché queste ultime hanno anche compiti di archiviazione delle chiavi private, preclusi invece alle prime. Così EUROPEAN COMMISSION, ***Ensuring Security and Trust in Electronic Communication*, cit.**

[19] L'inciso « se soggetti privati », contenuto nell'art. 8^3 lett. *a*, fa pensare che anche nel settore privato (dato che l'art. 8^3 fa salvo l'art. 17 relativo alla certificazione nell'ambito della p.a.) possono svolgere il ruolo di certificatori dei soggetti non privati.

[20] È previsto il riconoscimento delle firme verificabili con certificati rilasciati da certificatori stranieri (*cross certification*) operanti sulla base di licenza rilasciata da altro Stato membro dell'UE o dello Spazio economico europeo, subordinando tale riconoscimento alla dimostrazione di « equivalenti requisiti » di sicurezza (art. 8^4).

detti requisiti sembra essere compito dell'AIPA, in un regime di tipo *autorizzatorio* (licenza) e non concessorio (art. 8^4)[21].

In numerose leggi e progetti di legge stranieri e sovranazionali sulla materia, la struttura ed il quadro di funzionamento delle autorità di certificazione (*public key infrastructure*) sono puntualmente disciplinati su un piano legislativo e non regolamentare, prevedendo in maggioranza una struttura gerarchizzata a due livelli, con il livello sovraordinato (*root authority*) di emanazione statale o pubblica che certifica le autorità sottordinate, normalmente private. A tal proposito, le poche norme che il regolamento contiene in tema di autorità di certificazione dovranno, pertanto, necessariamente essere integrate dalle emanande regole tecniche *ex* art. 3. Sembra, fin d'ora, che con la scelta della forma della s.p.a. si sia inteso istituire un sistema di certificazione con soggetti imprenditori operanti in libera concorrenza[22]. Non è però ancora chiaro dal testo del regolamento, se i certificatori *ex* art. 8^3 rappresenteranno ognuno una singola autorità di vertice, oppure, se diversamente le loro chiavi pubbliche dovranno essere a loro volta certificate dall'AIPA, che svolgerebbe così il ruolo di unico certificatore di vertice per il territorio nazionale[23]. Non è neanche prevista una gerarchizzazione dei certificatori con autorità sottordinate certificate dai soggetti previsti dall'art. 8^3.

5. I CERTIFICATI.

In sede di emissione del certificato (art. 8^1), il certificatore, previo *accertamento dell'identità personale* del richiedente, « garan-

[21] Il regolamento non impedisce l'impiego di firme digitali certificate da parte di soggetti non autorizzati, e l'utilizzo di sistemi di cifratura (algoritmi) diversi da quelli che verranno riconosciuti dalle emanande regole tecniche. In queste ipotesi, poiché il regolamento (artt. 5^1, 8^1, 2 e 3), non permette di attribuire al documento informatico l'efficacia di scrittura privata *ex* 2702 c.c., si dovrebbe rientrare, pertanto, nella generale categoria del semplice documento informatico, con il valore di riproduzione meccanica *ex* art. 2712 c.c. (art. 5^2). Effetti probatori maggiori potranno, peraltro, derivare dall'esistenza di sottostanti accordi contrattuali, eventualmente rafforzati dal deposito della chiave pubblica presso un notaio. Vedi R. ZAGAMI, ***Firme « digitali »*, 1996, cit., p. 163 e p. 159 s. Utah DSA ammette espressamente le firme digitali certificate da AC non autorizzate (46-3-201, n. 6), ma esclude che si verifichino le presunzioni di provenienza della firma: spetterà quindi all'attore dare la relativa prova. L'attribuzione di valore probatorio ad una firma digitale sulla base di accordi contrattuali precedentemente stipulati tra mittente e destinatario del messaggio è prevista da UNCITRAL, *Model Law on Electronic Commerce*, cit., art. 13.**

[22] Essenziale al ruolo di certificatore è la sua indipendenza e terzietà rispetto agli interessi coinvolti nelle transazioni. Un sistema di certificatori privati con scopo di lucro potrebbe non garantire sufficientemente questa esigenza, potendosi prospettare delle ipotesi di conflitto di interessi. D'altra parte, è impraticabile un obbligo di astensione, una volta che una firma digitale è stata apposta, in relazione ad un certificato già emesso; resta, ovviamente, la responsabilità per i danni (art. 9) che il certificatore può avere causato violando la sua posizione di terzietà.

[23] Presumibilmente, i certificati delle chiavi pubbliche proprie dei certificatori

tisce la corrispondenza biunivoca tra chiave pubblica e soggetto » (art. 1 lett. *h*, art. 9^2 lett. *a*)[24]. Inoltre, considerando che si tratta di una tecnologia ancora relativamente nuova, il certificatore è tenuto ad informare i richiedenti sugli aspetti tecnici della procedura di certificazione (art. 9^2 lett. *e*)[25]. Sembra che nessun ruolo sia affidato al notaio in sede di emissione dei certificati; le procedure e le attività di certificazione, anche riguardo alla fase dell'accertamento dell'identità personale e della dichiarazione di corrispondenza tra chiave e soggetto, sono, infatti, riservate ai certificatori autorizzati (art. 1 lett. *h* e lett. *k*, art. 8, art. 9^2 lett. *a*)[26].

Per quanto riguarda il contenuto dei certificati, si ricava dal regolamento l'indicazione delle generalità di una persona, della corrispondente chiave pubblica e del termine di scadenza (art. 1 lett. *h*). Ulteriore contenuto minimo dovrà essere anche l'indicazione di un numero seriale identificativo, dell'algoritmo di cifratura da utilizzare, del periodo di validità (*operational period*) (o dell'eventuale revoca), del certificatore ed, infine, la *firma digitale* di quest'ultimo applicata su tutti gli elementi precedenti. Altre informazioni indicabili (le c.d. *certificate extensions*) sono eventuali poteri di rappresentanza volontaria, legale od organica (ad es. l'amministratore delegato di una società, oppure l'indicazione che le chiavi sono da usare con « firma congiunta », o con « firma disgiunta »), titoli e cariche professionali (art. 9^2 lett. *c*)[27]; non è

(necessari per la verifica dei certificati da loro stessi emessi) saranno reperibili dall'« apposito elenco pubblico, consultabile in via telematica », dove saranno inclusi i certificatori stessi (art. 8^3).

[24] È imprescindibile anche un accertamento dello stato di capacità legale e naturale del richiedente (ad es. interdizione, fallimento, ecc.) (art. 9^2 lett. *h*).

[25] Il rapporto tra titolare della chiave e certificatore può essere ricostruito in termini contrattuali (così espressamente Utah DSA), in quanto soggetti privati ed operanti in regime di libera concorrenza come imprese commerciali. Nel contratto, l'utente accetta il certificato, e si definiscono quegli aspetti che possono essere diversi tra i vari certificatori e che vanno oltre le prescrizioni legislative ed i requisiti minimi comuni (ad es. costi, qualità del servizio, limiti di responsabilità, livelli di sicurezza). Il contratto in questione dovrebbe essere concluso in forma scritta su carta (a meno che il richiedente non possieda già altra valida chiave privata con cui sottoscrivere) e contenuto nel relativo certificato oppure da questo richiamabile mediante link ipertestuale alle condizioni generali contrattuali del certificatore (*certification practice statement*).

[26] Nelle leggi e progetti di certi Stati americani, i *public notaries* agiscono come autorità certificanti subordinate, o come loro supporto.

[27] Le chiavi con le quali agiscono gli enti sono comunque intestate a persone fisiche, la cui autorizzazione ad agire ed i poteri di *rappresentanza organica* risultano dai certificati, in cui andrebbero incorporate (eventualmente *per relationem* con links telematici ipertestuali) le disposizioni rilevanti degli statuti; eventuali discordanze tra le risultanze dei certificati e quelle dei registri tradizionali (ad es. con riguardo alla sussistenza ed ai limiti dei poteri di rappresentanza) andrebbero risolte con la prevalenza dei secondi (ad es. registro delle imprese), almeno fino a quando non si stabilisca un collegamento diretto tra gli archivi dei certificati ed i registri già esistenti, per cui, ad es. una modifica degli amministratori nel registro delle im-

previsto che siano indicati limiti di utilizzo entro valori prestabiliti o per tipi di atti[28].

A differenza delle chiavi private[29], le chiavi pubbliche sono destinate ad essere divulgate e rese pubbliche (art. 1 lett. *f*, art. 8^1) ed a tal scopo è stabilita l'istituzione di appositi « registri su cui essa [la chiave pubblica] è pubblicata per la consultazione » (art. 10^7)[30] da

prese, porta ad un automatico aggiornamento dei primi. In caso di *rappresentanza volontaria*, la procura andrebbe incorporata (eventualmente *per relationem*) al certificato; per l'efficacia delle modificazioni o della revoca della procura *ex* art. 1396 c.c. occorrerà anche intervenire sul relativo certificato; la revoca del certificato non comporta revoca tacita della procura (art. 1724 c.c.); in caso di discordanza tra contenuto del certificato e procura sarà quest'ultima a prevalere. In caso di *rappresentanza legale*, rispetto al contenuto dei certificati, saranno prevalenti le risultanze del registro delle tutele e di quello delle curatele (artt. 47-51 att. c.c.).

[28] Per Utah DSA, il certificato può contenere un *recommended reliance limit*, cioè l'indicazione di un limite di responsabilità per il certificatore, un avviso per coloro che fanno affidamento sul certificato, che il valore dei risarcimenti che ne possono derivare non superino la somma indicata (sec. 46-3-309). Si tratta sostanzialmente di una limitazione contrattuale di responsabilità *ex* art. 1229 c.c., eventualmente collegata ad un massimo numero di certificati che possono essere richiesti in un certo periodo di tempo, al fine di evitare che il limite stabilito per la singola transazione possa essere moltiplicato indefinitamente per le transazioni compiute.

[29] Non si prevede un sistema di *key escrow* o *key recovery* . La chiave privata è « destinata ad essere conosciuta soltanto dal soggetto titolare » (art. 1 lett. *e*), ed il certificatore è tenuto a non rendersi depositario di chiavi private (art. 9^2 lett. *g*). Al contrario, il primo schema di regolamento (settembre 1996) prevedeva un archivio dove registrare anche le chiavi private (art. 27). In un sistema di *key escrow* una copia della chiave privata è depositata presso un'autorizzata TTP; la copia può anche essere suddivisa in due o più parti da depositare presso più TTPs. In un sistema di *key recovery* la chiave privata non è copiata e depositata fin dall'inizio: il sistema di criptazione permette però ad istituzioni autorizzate, come le TTPs, di ricostruire la chiave privata su richiesta. Una volta che la chiave è ricostruita non vi è quindi alcuna differenza con il sistema di *key escrow*, dato che entrambi permettono l'accesso alle informazioni criptate. La certificazione tecnicamente si riferisce solo alle chiavi pubbliche (art. 1 lett. *h*) e non anche a quelle private e, pertanto, l'archiviazione centralizzata di quest'ultime non è assolutamente necessaria per ottenere i risultati della certezza dell'integrità e della provenienza. Attribuire a soggetti diversi dai legittimi titolari, la conoscenza delle chiavi private, comporterebbe una generale situazione di rischio legata alla conservazione di tali chiavi, contro basilari principi di certezza del diritto e senza possibilità di pretese giustificazioni fondate su esigenze di ordine pubblico. In questo senso vedi anche OCSE, *Guidelines*, cit.; UNCITRAL, *Planning*, cit., par. 20. Diversi sono, invece, i termini del problema nel caso della cifratura a scopo di segretezza (vedi il dibattito in corso negli USA in ordine alla proposta del governo federale circa l'introduzione dell'*Escrowed Encryption Standard*, implementato nel « clipper chip », il quale attraverso una *escrowed key* permette ad organismi pubblici autorizzati la decifrazione delle comunicazioni). In ragione di ciò, i sistemi di validazione (*hardware* e *software* per la gestione delle firme digitali) dovranno normalmente impedire l'uso delle chiavi a scopo di segretazione.

[30] Gli archivi dei certificati conterranno, evidentemente, una serie di dati personali, pertanto, l'art. 9^2 lett. *f* impone ai certificatori di attenersi alle norme per il loro trattamento (l. 675/1996 e successive modifiche), tra cui rientra anche l'art. 15 (relativo alle misure minime di sicurezza da adottare in via preventiva) richiamato, peraltro, dall'art. 3^4 del regolamento. Comunque, il consenso espresso dell'interessato non sembra necessario, in applicazione dell'art. 12 lett. *b* e lett. *c* della l. 675. Le implicazioni che gli archivi dei certificati possono avere per la privacy sono riconosciute anche in OCSE, *Guidelines*, cit., e UNCITRAL, *Planning*, cit. D'altronde, in generale, l'impiego delle firme digitali potrebbe semplificare notevolmente e ridurre i costi per l'implementazione di tutte le formalità richieste dalla legge n. 675.

potersi effettuare in forma telematica (art. 8^2). Lo stesso certificatore che ha certificato la chiave provvede alla sua conservazione per un periodo non inferiore a 10 anni dall'inizio di validità (art. 8^2), mediante l'istituzione ed il mantenimento di un archivio telematico dei certificati (*key repository*): da ogni firma digitale si dovrà poter ricavare il certificatore da consultare per la verifica della stessa (art. 10^7), che dovrà avvenire auspicabilmente in modo automatico[31]. La consultazione telematica dei certificati (e delle liste dei certificati revocati) è una condizione essenziale per la funzionalità dell'intero sistema, data la normale esigenza di una verifica rapida (in tempo reale al momento della loro apposizione) delle firme digitali, per accertare la sussistenza di eventuali revoche o scadenze[32]. Se il destinatario di un messaggio decide di non fidarsi della firma digitale del mittente (ad es. perché revocata), deve a lui dichiararlo prontamente (Utah DSA sec. 46-3-402 e, probabilmente, artt. 1337 e 1338 c.c.).

Per la diffusione delle chiavi pubbliche delle autorità certificatrici di vertice, indispensabili per la verifica dei certificati da loro stesse emessi, occorrerebbe prevedere una divulgazione con mezzi diversi e più sicuri (ad es. pubblicazione in G.U. o mediante CD-WORM appositamente stampigliati) per scongiurare i rischi di diffusione di chiavi false, dato che tali chiavi non possono essere verificate perché non certificabili, se non da autorità di pari grado[33].

6. Firma digitale autenticata.

L'autenticazione di firma digitale si giustifica qualora si riconosca che la funzione dell'autentica non si esaurisce nella mera certificazione della provenienza soggettiva[34], ma comporta anche

[31] L'art. 9^1, prevedendo la responsabilità civile nell'uso dei sistemi di firma digitale, tipizza una serie di obblighi a carico dei certificatori e considera sostanzialmente l'uso di tali sistemi come esercizio di attività pericolosa per sua natura (art. 2050 c.c.), in quanto impone al certificatore di provare (« è tenuto ») di aver adottato tutte le misure tecniche ed organizzative idonee ad evitare danno. Un'ulteriore responsabilità, di tipo contrattuale, potrebbe configurarsi qualora si ricostruiscano in tal senso i rapporti tra i titolari delle chiavi ed i certificatori.

[32] Nel caso di comunicazioni in reti aperte ed insicure (come Internet) vi è comunque il rischio del *man in the middle attack*. Un terzo si potrebbe inserire nella comunicazione e sostituire il certificato inviato dal certificatore con un altro certificato verificabile con la stessa chiave pubblica del certificatore, però emesso in un periodo anteriore alla sua perdita di validità.

[33] Le chiavi delle autorità di vertice non possono, infatti, essere fornite telematicamente, a meno che il sistema di trasmissione dati non sia assolutamente sicuro da intrusioni (situazione normalmente improbabile nelle reti aperte, come Internet).

[34] L'autentica di una firma digitale può, infatti, apparire superflua se ad essa si assegna solo la funzione di accertamento della provenienza soggettiva del documento informatico. Una tale certezza è, infatti, evidentemente raggiungibile di per sé mediante la verifica del certificato, già emesso previo accertamento dell'identità personale del richiedente (art. 1 lett. *h* e art. 9^2 lett. *a*). In tal senso, per Utah DSA, le firme di-

un controllo di legalità da parte del notaio sul contenuto del documento informatico sottoscritto[35]. In tale prospettiva, l'art. 16 prescrive che il pubblico ufficiale autenticante attesti, oltre il fatto che « la firma digitale è stata apposta in sua presenza » (artt. 2703^2 c.c. e 72 l. not.)[36], che « il documento sottoscritto risponde alla volontà della parte [art. 47^3 l. not.] e non è in contrasto con l'ordinamento giuridico ai sensi dell'articolo 28, numero 1, della legge 16 febbraio 1913, n. 89 (legge notarile) »[37].

Il notaio o altro pubblico ufficiale sottoscrive l'autentica apponendo la propria firma digitale (art. 16^3)[38], la quale sostituisce « la apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti » (anche art. 10^6). In considerazione del loro superiore grado di importanza, è stabilito che la certificazione e pubblicazione delle chiavi pubbliche dei notai e degli altri pubblici ufficiali non appartenenti alla p.a. è compiuta in modo autonomo da soggetti diversi dai certificatori *ex* art. 8^3, e con modalità che verranno individuate da successive leggi e regolamenti (art. 17^3).

In una prospettiva di simmetria tra documentazione cartacea e documentazione informatica[39], la firma digitale autenticata ai

---

gitali sono « *self-authenticating* »; è detto però espressamente che ciò è vero solo nella prospettiva *dell'american notary* e non dei notai di *civil law*, i quali sono tenuti ad effettuare un controllo della legalità del contenuto (*Commentary to the Utah DSA*, sec. 46-3-405). Comunque, l'autentica fornisce una maggiore garanzia che la firma digitale è stata apposta personalmente dal titolare, e non da altri, con o senza autorizzazione.

[35] Per l'applicabilità dell'art. 28 l. not. alle scritture private autenticate è la maggioranza della dottrina notarile (vedi, tra i tanti, P. Boero, ***La legge notarile commentata*, Torino, 1993, p. 169 ss.; G. Casu, *L'atto notarile tra forma e sostanza*, Milano, 1996, p. 389 s.) e la giurisprudenza (Cass. civ. n. 2699/1994); *contra* Cass. pen. n. 2720/1990. Nel codice deontologico approvato dal Consiglio Nazionale del Notariato il 24 febbraio 1994 è stabilito che il notaio deve « controllare la legalità del contenuto della scrittura e la sua rispondenza alla volontà delle parti » (b.3). Un disegno di legge approvato dal Consiglio dei Ministri il 29 novembre 1997 prevede l'espressa estensione dell'art. 28 l. not. alle scritture private.**

[36] Considerando la *ratio* della prescrizione della « presenza », questa potrebbe in futuro ritenersi ugualmente soddisfatta da una *presenza virtuale* realizzata mediante avanzati sistemi di videoconferenza, in modo che il notaio possa, anche a distanza, indagare la volontà del « comparente », accertarsi della sua identità personale e del fatto che la firma digitale sia stata effettivamente apposta da lui stesso e non da altri.

[37] È, inoltre, richiesto al pubblico ufficiale di effettuare un accertamento dell'identità personale del sottoscrittore e della validità della chiave utilizzata (artt. 16^2 e art. 2703^2 c.c.) e perciò ne deriva che potranno essere autenticate solo firme validamente certificate.

[38] Struttura simile a quella dell'autentica *ex* art. 16, eccetto che per la mancanza del controllo di legalità *ex* art. 28 l. not., presentano i *transactional certificates* (ABA, *Guidelines*, cit., 1.34), emessi in relazione ad una o più specifiche firme digitali già apposte ed incorporate nel certificato stesso. Essi si contrappongono ai già esaminati certificati (*identifying certificates)*, i quali invece associano una chiave pubblica ad un'identità personale e sono utilizzabili per una molteplicità indefinita di future firme digitali.

[39] Secondo la *Relazione* al regolamento, « il criterio adottato, per la formulazione delle norme autorizzate, consiste nel tentativo di adattare le norme vigenti (in particolare la disciplina in materia di efficacia probatoria degli atti e dei documenti del codice civile) alle nuove realtà informatiche e telematiche ».

sensi dell'art. 16, si considera come riconosciuta ai sensi dell'art. 2703 c.c. e farà, dunque, piena prova della provenienza delle dichiarazioni da chi ha sottoscritto il documento informatico, anche se colui contro il quale è prodotto non riconosce la sottoscrizione, salvo l'esperibilità della querela di falso (art. 2702 c.c.)[40]. Le conseguenze di tale equiparazione sono straordinarie, in quanto potrebbero essere stipulati in *originale* ed in forma *esclusivamente informatica*, quasi tutti gli atti giuridici ammessi nel nostro ordinamento, con esclusione di quelli per i quali è richiesta la forma minima dell'atto pubblico. E gli atti così stipulati potranno essere direttamente immessi nei registri immobiliari (art. 2657 c.c.)[41] e nel registro delle imprese (art. 2189^2 c.c.)[42], anche mediante trasmissione telematica *in via definitiva* della richiesta (nota o domanda) e del titolo[43].

Poiché il documento informatico (art. 1 lett. *a*) è idoneo ad essere rappresentato non solo per testi, ma anche immagini, filmati, suoni ed in generale qualunque informazione digitalizzabile, ne deriva la configurabilità di *scritture private non testuali*. In perfetta applicazione del regolamento non si può negare che costituisca forma *scritta* (art. 4^1) e soddisfi letteralmente i requisiti richiesti dall'art. 1350 c.c. (art. 5^1), un documento informatico, con autentica notarile, recante la registrazione digitale audio e video (eventualmente completata anche da elementi testuali) della conclusione di un negozio (da trascrivere mediante indicizzazione non automatica del contenuto). Nuove prospettive si aprono anche per la forma del testamento, per cui accanto a quello olografo, potrebbe così assumere valore quello nuncupativo[44].

---

[40] In considerazione dell'espresso richiamo all'art. 2703 c.c. è da ritenere che l'autentica prevista dall'art. 16 costituisca una modalità *dell'autentica di tipo c.d. formale*, utilizzabile anche per autenticare negozi giuridici; a differenza degli altri due tipi di autentica (amministrativa e minore). Vedi G. CASU, ***L'atto notarile*, cit., p. 386.**

[41] Attualmente « la formalità si intende richiesta quando viene presentato in conservatoria [...] il titolo relativo [su carta], anche se la produzione del supporto informatico o la trasmissione telematica sia avvenuta in precedenza » (art. 1^3 d.m. 29/4/97). L'art. 10^{19} del d.l. 323/1996 stabilisce che il richiedente la formalità, « fermo restando l'obbligo di presentare [...] il titolo nelle forme previste dal codice civile, può altresì produrre il contenuto del titolo stesso su supporto informatico ».

[42] Il regolamento di attuazione (d.p.r. 581/1995) all'art. 8 della l. 580/1993, prevede il rilascio telematico dei certificati (art. 2 lett. *d*) e la possibilità di presentare la domanda anche su supporto informatico (art. 11), ma non anche la trasmissione telematica della domanda, ritenendo la Commissione che ha redatto il regolamento di escludere tale possibilità per la necessità di autenticazione posta dal codice civile.

[43] Vedi R. ZAGAMI, ***Firme « digitali »*, 1996, cit., p. 169.**

[44] Con le firme digitali, la funzione del notaio non è sminuita, ma piuttosto è richiesta nei suoi compiti di maggior valore professionale (funzione di adeguamento e controllo di legalità). Mentre, per converso, l'intervento notarile diventerebbe eccessivo per i compiti di mera certificazione, nei casi in cui l'autentica è richiesta esclusivamente ai fini di un controllo della provenienza soggettiva (autentica non negoziale), poiché sarebbe perfettamente funzionale una firma digitale anche non autenticata.

7. *Segue*: CYBERNOTARY.

Il compito di autenticare firme digitali è attribuito al *cybernotary*, una nuova figura di professionista nell'ordinamento statunitense, delineato nell'ambito dell'American Bar Association (ABA) e implementato per la prima volta con legge nello stato della Florida[45], la cui istituzione deriva dalla diversità di tradizioni giuridiche tra i sistemi di *common law* e quelli di *civil law* e, quindi, dall'esigenza (ancora più sentita in presenza di una documentazione informatica) di rendere i documenti giuridici provenienti dai primi accettabili nei secondi[46].

Come è noto, l'ordinamento statunitense non conosce la figura del notaio quale è nei paesi di *civil law*, come l'Italia. Il *public notary* è un mero certificatore e non ha alcun dovere di verificare la conformità alla legge del contenuto dell'atto che gli è sottoposto per l'autenticazione. Il *cybernotary*, invece, avrà il compito di assicurare la legalità dei documenti destinati all'estero (*authentication*), affinché essi non siano respinti dall'ordinamento destinatario, costituendo, pertanto, un ponte tra due tradizioni giuridiche (sec. 7 legge della Florida). Per svolgere correttamente i suoi compiti, il *cybernotary* dovrà essere scelto tra avvocati abilitati ad esercitare, dovrà possedere conoscenze di diritto straniero e di informatica e telematica con particolare riguardo ai sistemi di firma digitale (sec. 5)[47].

8. ATTI PUBBLICI NOTARILI.

Il regolamento non prevede la redazione di un atto pubblico notarile *originale* in forma informatica. L'efficacia probatoria privilegiata, le particolarità e complessità della legge notarile (l. 89/1913) e della l. 15/1968, hanno evidentemente sconsigliato, quantomeno nella prima fase di applicazione, tale possibilità. Inoltre, per la conclusione degli atti notarili, l'utilità della firma digitale

[45] *Electronic Commerce Act*, cit.; anche lo stato dello Utah ha redatto un progetto di *Act on Electronic Notarization* (HB 95 del 1997). Nella legge della Florida si è preferito usare la diversa locuzione di *international notary*, in quanto l'uso delle firme digitali e degli strumenti informatici da parte di questi nuovi professionisti è opzionale. Vedi FLORIDA DEPARTMENT OF STATE - DIGITAL SIGNATURE ADVISORY COMMITTE, **Electronic Commerce in Florida, 30 novembre 1996, in Internet.**

[46] Vedi M. MICCOLI, ***Cybernotary*, in *Notariato*, 1996, p. 105 ss.**; T. S. BARASSI, ***The Cybernotary: Public Key Registration And Certification And Authentication Of International Legal Transaction*, 1996, in Internet; ABA, *Resolution concerning the CyberNotary: an International computer-transaction specialist*, 2 agosto 1994.**

[47] Il regolamento non istituisce, evidentemente, una nuova figura di *cybernotary*, in quanto le sue funzioni di autenticazione sono già per tradizione secolare patrimonio del notariato italiano.

è minore, dato che essi non potrebbero comunque essere conclusi telematicamente, poiché, a differenza delle scritture private autenticate, è richiesta la contestuale presenza delle parti davanti al notaio per la lettura e sottoscrizione[48]. L'utilità si ripresenta quando occorre duplicare o trasmettere telematicamente il documento pubblico già concluso. Pertanto, non potrà essere redatto un atto pubblico *originale* in forma informatica, però potrà essere fatta una copia informatica di un atto pubblico redatto su carta. È, infatti, stabilito che i documenti informatici contenenti *copia* di un atto pubblico, se spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia probatoria ai sensi dell'art. 2714 c.c., e cioè « fanno fede come l'originale », se ad essi è apposta la firma digitale di colui che li spedisce o rilascia (art. 6^2). La produzione o esibizione dell'originale cartaceo non è richiesta, essendo sufficiente ad ogni effetto di legge, la sua copia informatica (art. 6^4)[49].

La piena validità delle copie informatiche degli atti pubblici offre, comunque, già di per sé vastissime prospettive di applicazione. Sarà possibile trasmettere telematicamente un atto pubblico, mantenendone la fede privilegiata, previa effettuazione di una copia informatica[50] (ad es. un notaio potrebbe ricevere telematicamente da un altro notaio una procura speciale da allegare all'atto pubblico ai sensi dell'art. 51, n. 3 della l. not.)[51]; i notai potranno consegnare in forma esclusivamente informatica le copie degli atti pubblici (ad es. un *floppy*, oppure la trasmissione di un messaggio *email*); inoltre, dalla copia informatica di un atto pubblico si potranno ricavare duplicati con piena efficacia probatoria, *senza che necessiti un nuovo intervento del notaio* depositario dell'originale cartaceo; e con tali copie in forma informatica si potranno, naturalmente, richiedere modificazioni nei registri immobiliari e delle imprese.

---

[48] Vedi in tal senso, tra gli altri, G. CASU, *L'atto notarile*, cit., p. 266 s.; DI FABIO, *Manuale di notariato*, Milano, 1981, p. 156.

[49] La sussistenza di un originale cartaceo dovrebbe essere funzionale anche alla risoluzione di eventuali controversie che potrebbero derivare dall'applicazione di una normativa ancora nuova e sperimentale. In mancanza dell'originale cartaceo dell'atto pubblico potrebbe, comunque, riconoscersi piena efficacia probatoria alla sua copia digitale in base all'art. 2716 c.c.

[50] Alla trasmissione telematica non andrebbero, naturalmente, applicate le complesse procedure stabilite dall'art. 71 l. not. previste per la trasmissione per telegrafo o per telefono. Inoltre, il documento ricevuto telematicamente ha la stessa efficacia probatoria dell'*originale* trasmesso e non l'efficacia più limitata prevista dall'ult. comma del medesimo art. 71, per il quale « le comunicazioni telegrafiche o telefoniche come sopra accertate, si *presumono* conformi agli atti originali fino a prova contraria ».

[51] Il regolamento prevede l'allegazione di una copia informatica di un documento in origine cartaceo (art. 16^4), mentre non prevede l'ipotesi speculare di allegazione di un documento informatico ad un atto pubblico cartaceo. Il notaio dovrà riprodurne il contenuto su carta ed attestare la sua conformità all'*originale* informatico.

L'art. 7 prevede che il titolare può ottenere il deposito in forma segreta della chiave privata con le modalità e nelle forme[52] di cui all'art. 605 c.c. (testamento segreto)[53]. La *ratio* va individuata, prevalentemente con riferimento alla cifratura a scopo di segretezza, nell'esigenza di conservare in modo segreto e sicuro una chiave privata, per evitare gli inconvenienti conseguenti ad una sua perdita (ad esempio per smarrimento della *password* di accesso o per cancellazione del supporto dove è conservata)[54], dato che non è prevista una memorizzazione presso archivi centralizzati per eventuali recuperi (art. 9^2 lett. *g*). In secondo luogo, con il deposito, si potrebbe precostituire un elemento di prova ulteriore a quello della certificazione, per la risoluzione di eventuali controversie. D'altra parte, non è escluso che il deposito *ex* art. 605 c.c. si riferisca anche a chiavi non certificate o comunque non conformi a quelle che saranno individuate dalle emanande regole tecniche[55].

9. Validazione temporale.

È definita « validazione temporale, il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici una data ed un orario opponibili ai terzi » (art. 1 lett. *i*). Tecnicamente, si tratta di apporre una data ed un'ora ad un documento informatico (di qualunque contenuto: testi, suoni, immagini, ecc.) e di sigillare il tutto con la firma digitale (rinnovabile nel tempo) di una terza parte fidata, che il regolamento non individua (rinviando alle regole tecniche *ex* art. 3^1)[56]; giuridicamente,

[52] La chiave da depositare « può essere registrata su qualsiasi tipo di supporto idoneo » (art. 7^2) e quindi potrebbe essere trascritta su un foglio di carta, oppure su supporto digitale, come ad es. un CD-ROM od un *floppy disk* .

[53] Per l'art. 67 l. not. il notaio può rilasciare copia della chiave privata depositata solo al depositante medesimo o a persona munita di procura speciale autenticata. Inoltre, per l'art. 608 c.c., il testatore, o meglio il depositante, (e nessun altro) può in ogni tempo ritirare la chiave privata dalle mani del notaio presso il quale è depositata.

[54] Per Utah DSA, il titolare può comunicare la propria chiave privata (ad es. per servizi di *key recovery* in caso di smarrimento) all'AC, la quale la detiene come fiduciario (trustee), non può utilizzarla senza il consenso del titolare (sec. 46-3-305, 3) ed è responsabile secondo le norma del trust (*Digital Signature Act: Examples*).

[55] L'art. 7 del regolamento si riferisce espressamente al deposito in forma segreta della sola chiave privata, in quanto è evidente che una tale esigenza di segretezza non si pone, invece, per la *chiave pubblica*. Quest'ultima potrebbe, peraltro, essere depositata ai sensi dell'art. 61 della l. not. che prevede in generale il deposito di atti presso il notaio, il quale di conseguenza, dovrà rilasciarne copia a chiunque la richieda (art. 67 l. not.). Il deposito della chiave pubblica, unitamente a preventivi accordi contrattuali tra gli interessati, consentirebbe di limitare i rischi nell'utilizzo delle chiavi non certificate (o non certificabili perché non conformi agli standards che verranno riconosciuti), realizzando una sorta di rudimentale sistema alternativo di certificazione delle chiavi.

[56] Il servizio di validazione temporale (*time-stamping*) rientra nei cosiddetti *ancillary services* (*key repository*, *escrow service*, *confirmation service*, *key generation service*, *ecc.*), i quali possono essere

si realizza sostanzialmente l'effetto civilistico della registrazione degli atti già svolta dagli uffici del registro (art. 2704 c.c. e art. 18 d.p.r. 131/1986).

Nell'autenticazione *ex* art. 16 è già ovviamente ricompresa una validazione temporale (art. 2704 c.c.), la quale rappresenta un *minus* rispetto alla prima, dato che non presuppone l'esistenza di una scrittura privata e non comporta alcun indagine sulla volontà ed identità dei sottoscrittori e sul contenuto dell'atto. In mancanza di un'autenticazione *ex* art. 16, e mancante anche una validazione temporale, la data di un documento informatico con firma digitale (in quanto scrittura privata *ex* art. 5^1) potrà essere accertata ai sensi dell'art. 2704 c.c. (ma in certi casi solo fino a quando non è scaduta, revocata o sospesa la relativa chiave)[57].

10. Scadenza, revoca e sospensione delle chiavi.

La chiave può perdere « validità » (art. 1 lett. *n*), a seguito della scadenza prestabilita, oppure di revoca (art. 1 lett. *l*) o sospensione (art. 1 lett. *m*)[58] nei casi « di perdita del possesso della chiave [privata], di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare [ad es. fallimento, morte, interdizione, ecc.], di sospetti abusi o falsificazioni »[59] (art. 9^2 lett. *h*), che possono riguardare il titolare, la chiave privata o i sistemi informatici del certificatore. La revoca o sospensione è disposta, su « richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo »[60] (art. 9^2 lett. *h*), oppure anche senza il consenso del titolare (ad es. per le cause limitative della capacità, o in caso di falsità o di compromissione della sicurezza dei certificati), ed è operata dallo

svolti dagli stessi certificatori o da soggetti diversi.

[57] Mancante una validazione temporale e mancante anche un'autentica notarile, nei casi di « morte o sopravvenuta impossibilità fisica » previsti dall'art. 2704 c.c., l'accertamento dell'anteriorità della data è consentito solo fino a quando non è scaduta (salvo rinnovazione), revocata o sospesa la relativa chiave.

[58] La sospensione dovrebbe essere una misura cautelare e strumentale, da adottarsi con urgenza nei casi in cui non sia prontamente accertabile il fondamento dei presupposti per la revoca. In seguito, il certificatore farà le opportune indagini che potranno condurre alla revoca (definitiva) oppure al ripristino di validità del certificato. Pertanto, durante il periodo di sospensione (non eccedente le 48 ore secondo il DSA dello Utah sec. 46-3-302) si deve mantenere la segretezza della chiave privata.

[59] L'impiego della chiave privata da parte di persona diversa dal titolare, ma da questi autorizzata, realizza una sostituzione soggettiva inquadrabile in una sorta di rappresentanza diretta, poiché gli effetti degli atti si ripercuotono direttamente in capo al titolare della chiave, anche in mancanza dell'esternazione della procura (eventualmente tacita); fermo restando che il meccanismo normale di rappresentanza presuppone, comunque, l'impiego della firma digitale del rappresentante e non quella del solo rappresentato.

[60] Si pensi al caso di revoca di una procura o di cessazione delle funzioni di un rappresentante legale o organico.

stesso soggetto che ha emesso il certificato (art. 10^4); deve essere motivata e pubblicata (art. 10^5) per essere verificabile telematicamente ai fini della sua efficacia ed opponibilità.

Una firma digitale apposta o associata mediante una chiave scaduta, oppure revocata o sospesa (e correttamente pubblicata) equivale a mancata sottoscrizione (art. 10^5) e, pertanto, qualora la forma scritta è richiesta *ad substantiam*, il relativo atto giuridico è nullo o inesistente. In caso di atti bi- o plurilaterali, o che possono produrre effetti nella sfera giuridica altrui, nessun affidamento incolpevole o indennizzo può essere riconosciuto in capo alla controparte o al terzo, i quali hanno la possibilità e l'*onere* di consultare i registri telematici per informarsi sulla validità della chiave[61].

È stabilito che la revoca non ha efficacia retroattiva (art. 1 lett. *l*), tuttavia, per mantenere *l'efficacia probatoria dei documenti validamente sottoscritti in un momento anteriore* alla scadenza, revoca o sospensione, occorre la dimostrazione che la firma digitale sia stata apposta durante il periodo di validità della chiave (*operational period*); altrimenti, dal momento della scadenza, revoca o sospensione (regolarmente pubblicate *ex* art. 10^5), perdono efficacia anche tutti i documenti anteriormente (e validamente) sottoscritti con la relativa chiave privata, in quanto non può più essere escluso il rischio che il documento sia stato sottoscritto da un usurpatore (perché ha decifrato chiavi non più sicure o si è impossessato di chiavi altrui).

L'efficacia probatoria di documenti sottoscritti con firme digitali verificabili con chiavi e certificati che hanno perso validità, può essere mantenuta[62] con l'intervento di un terzo garante, che sostanzialmente attesta l'anteriorità della firma rispetto agli eventi che ne hanno determinato la perdita di validità[63]; intervento che potrebbe realizzarsi, quale *onere* a carico degli interessati e, comunque durante *l'operational period*, con una duplice modalità[64]:

[61] Non si può propriamente parlare di successiva *ratifica* (art. 1399 c.c.) o *convalida* (art. 1444 c.c.) dell'atto firmato con chiave non più valida, dato che si tratterebbe dell'apposizione di una firma ad un atto prima inesistente o nullo e non solo inefficace o annullabile.

[62] Tale esigenza è particolarmente rilevante per i documenti destinati ad essere conservati per lunghi periodi di tempo, dato che, mentre una sottoscrizione su carta, con il trascorrere del tempo, mantiene in via di principio lo stesso valore probatorio; una firma digitale, invece, è fin dall'inizio destinata a perdere sicurezza in breve tempo a causa dell'inarrestabile progresso nella potenza di calcolo degli elaboratori (il termine di scadenza della chiave non può essere superiore a 3 anni, art. 1 lett. *h*).

[63] Per consentire la verifica di firme scadute o, comunque, non più valide, è stabilito che le chiavi pubbliche siano conservate per almeno 10 anni dall'inizio della loro validità (art. 8^2).

[64] L'intervento del terzo garante è indispensabile perché i soggetti firmatari potrebbero verosimilmente non avere alcun interesse all'apposizione di una nuova firma digitale rinnovata, a meno che non venga stabilito un improbabile obbligo di ap-

a) affidamento dei documenti informatici (non solo dei loro *hash*) al terzo garante (ad es. archivi notarili o uffici del registro) che li custodisca, assicurando che non vengano alterati, e li consegni ai legittimati a riceverli, con l'apposizione della proprio *attuale* firma digitale a garanzia dell'autenticità;

b) validazione temporale (art. 1 lett. *i*)[65], la quale consentirà di mantenere l'efficacia probatoria almeno fino al momento in cui non perde validità anche la chiave con la quale è stata apposta la validazione; naturalmente, salvo possibilità di rinnovare (o confermare), anche più volte, la stessa validazione con una nuova (attuale) firma del terzo garante[66].

12. Firma digitale falsa.

Nello stabilire le conseguenze giuridiche che ricadono su colui che risulta autore di una firma digitale, dopo la verifica del relativo certificato, si deve scegliere, in astratto, tra due opzioni di fondo: *a*) vincolatività, senza possibilità di eccepire l'incolpevole falsità della firma; *b*) vincolatività, con la possibilità di fornire, a certe condizioni, una prova contraria. Il regolamento adotta la prima soluzione, poiché l'effetto della revoca (o sospensione), cioè la « mancata sottoscrizione », si verifica solo dal momento della sua pubblicazione (art. 10^5). Prima di allora[67], salvo una limitata eccezione, il rischio *dell'impiego abusivo della chiave privata*[68] da parte di persona diversa dal tito-

porre una nuova sottoscrizione (la cui violazione porterebbe, comunque, all'apposizione della firma del terzo garante, con un meccanismo simile a quello dell'art. 2932 c.c.).

[65] Sulla necessità della validazione temporale per determinare se una firma digitale è stata apposta durante il periodo di validità (*operational period*) del certificato vedi ABA, *Guidelines*, cit., 1.33.2; UNCITRAL, *Planning*, cit., 38a.

[66] L'efficacia probatoria dei documenti con autentica notarile *ex* art. 16 (in quanto aventi data certa) è di per sé mantenuta almeno fino al momento in cui perde validità la firma del notaio, salvo possibilità di prolungarne la validità con una validazione temporale o con deposito presso un garante. In caso di revoca della chiave del notaio autenticante, il documento potrebbe valere come semplice scrittura privata informatica non autenticata *ex* art. 5^1, se le firme delle parti sono ancora valide (art. 2701 c.c.). Non sorgono, invece, problemi dalla revoca e scadenza delle chiavi private utilizzate per l'emissione dei certificati, in quanto questi vanno chiesti all'occorrenza direttamente al certificatore e sono automaticamente firmati con la chiave più recente, dato che non occorre che abbiano un valore probatorio protratto nel tempo; a meno che non si ammetta la revoca retroattiva per le chiavi dei certificatori.

[67] Il certificatore è tenuto a procedere tempestivamente alla revoca o sospensione e a darne immediata pubblicazione (art. 9^2 lett. *h* e lett. *i*). Se la pubblicazione è stata omessa o ritardata dal certificatore, su quest'ultimo si sposta il relativo rischio per i danni che ne sono eventualmente derivati, a meno che non provi di aver adottato tutte le misure idonee ad evitare il danno (art. 9^1).

[68] L'apposizione di firme digitali sotto nome *altrui* può derivare, oltre che dalla sottrazione di una chiave privata, anche dalla creazione di una nuova coppia di chiavi e dalla loro *falsa certificazione*, derivante da dolo o negligenza di un certifica-

lare[69] è posto sempre a carico di quest'ultimo, sul quale grava in sostanza una forma di *responsabilità oggettiva* per le conseguenze di tutti gli atti giuridici in forma informatica verificabili con la corrispondente firma digitale. Si pone, pertanto, una presunzione assoluta (*juris et de jure*) di riferibilità della firma digitale al soggetto titolare della chiave pubblica che risulta dal relativo certificato e non si ammette alcuna possibilità di fornire la prova contraria per sottrarsi alle conseguenze che derivano da un uso abusivo della chiave privata prima della richiesta di revoca (o sospensione). Pur riconoscendo al documento informatico l'efficacia di scrittura privata *ex* art. 2702 c.c. (art. 5^1) non si ammette il principio del disconoscimento previsto dallo stesso articolo[70]. Si produrranno, allora, in capo al titolare della chiave tutti gli effetti che derivano dall'atto giuridico compiuto dall'usurpatore[71], privilegiando una scelta di massima tutela dell'affidamento negoziale.

Come correttivo di queste gravi conseguenze è ammessa una limitata forma di *pubblicità di fatto*, per cui, è consentito (con l'onere a carico del revocante o di chi richiede la sospensione) provare che la revoca o sospensione era già a *conoscenza* delle parti interessate, anche in mancanza (o prima) della necessaria pubblicazione (art. 10^5)[72]. Tale prova, però, letteralmente, sembra poter sostituire solo la *mancata (o ritardata) pubblicazione*[73], ma non anche la mancata previa *richiesta* di revoca o sospensione al certificatore stesso; inoltre, sembra che non sia consentito dimostrare la sem-

---

tore, eventualmente risultante dall'utilizzo abusivo della sua chiave privata. Il regolamento non fa distinzioni, quindi, anche in tali ipotesi, prima della pubblicazione della revoca, sembra che l'atto firmato abusivamente produca comunque i suoi effetti, non essendo ammessa prova contraria da parte del titolare, ferma restando l'eventuale responsabilità del certificatore (art. 9), e quella dell'usurpatore (ove identificabile).

[69] L'uso abusivo di una chiave privata altrui ripropone in parte gli stessi problemi derivanti da una sottoscrizione (su carta) apocrifa. Vedi M. ORLANDI, ***La paternità delle scritture***, **Milano, 1997, p. 107 ss.**

[70] Se si considera la verifica positiva della firma digitale apposta, come equivalente al « riconoscimento » della sottoscrizione di cui all'art. 2702 c.c., potrebbe sostenersi, in base alla stessa norma (richiamata dall'art. 5^1) l'ammissibilità della *querela di falso*.

[71] Per favorire la diffusione del sistema delle firme digitali, si potrebbero porre a carico dei certificatori i rischi economici derivanti dall'uso abusivo delle chiavi private (nei casi in cui l'usurpatore non sia identificabile ed il certificatore stesso provi la sua mancanza di colpa), assegnando loro una sorta di funzione assicurativa, così come agiscono le società emittenti carte di credito, predeterminando un limite massimo di responsabilità per l'utente.

[72] La pubblicità della revoca della chiave privata ha *efficacia dichiarativa*, con il correttivo della pubblicità di fatto, in modo analogo a quanto è previsto per l'efficacia dell'iscrizione nel registro delle imprese (art. 2193 c.c.). La revoca della chiave è opponibile dal momento della pubblicazione (efficacia positiva); l'omessa pubblicazione della revoca non può essere opposta (efficacia negativa), salvo la dimostrazione dell'effettiva conoscenza.

[73] « La revoca o sospensione [...] hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che *essa* [cioè la revoca o sospensione] era già a conoscenza di tutte le parti interessate » (art. 5^2).

plice *conoscibilità* della revoca o sospensione, cioè l'ignoranza dipendente da colpa.

Soluzione diversa sarebbe stata la previsione di una presunzione *juris tantum* di provenienza e di integrità del documento, come stabilita in numerosi provvedimenti stranieri e sovranazionali sul tema[74]. È, infatti, ritenuto ingiusto che il titolare della chiave risponda oggettivamente anche quando per circostanze non attribuibili a sua colpa abbia perso la chiave e sia stato nell'impossibilità di effettuare una tempestiva denuncia. Naturalmente a lui farà carico la (spesso difficile) prova dell'impiego abusivo della chiave, ed il suo stato soggettivo di non colpevolezza che ha determinato l'abuso, cioè aver adottato le misure idonee a salvaguardare la sicurezza della chiave stessa. Inoltre, a tutela dell'affidamento, la possibilità di fornire la prova contraria dovrebbe essere subordinata alla malafede dell'altro contraente, intendendola come conoscenza o conoscibilità della falsità (invalidità) della firma (art. 1147 c.c.), secondo un principio generale del nostro ordinamento (vedi artt. 428, 1431, 1439[2], 1445 c.c.); malafede che andrebbe provata dalla persona che appare come sottoscrittore (art. 1147[3] c.c.). In caso di atti unilaterali si potrebbe richiedere la prova del grave pregiudizio all'autore (art. 428 c.c.)[75].

Ulteriore ipotesi è quella dell'uso di una chiave associata ad un nome *falso*, inesistente (la c.d. contraffazione per invenzione, contrapposta a quella per usurpazione)[76], che può derivare dall'uso abusivo di una chiave privata di un certificatore, o dall'emissione (con dolo o con colpa) di falsi certificati da parte di quest'ultimo. Il caso potrebbe inquadrarsi ed essere risolto nel tradizionale tema della conclusione del contratto sotto falso nome[77].

---

[74] ABA, *Guidelines*, cit., prevedono una presunzione di provenienza controvertibile, mediante inversione dell'onere della prova a carico di colui che appare come sottoscrittore (5.6); UNCITRAL, *Planning*, cit., prevede una presunzione, superabile dalla dimostrazione che il destinatario del messaggio conosceva o avrebbe potuto conoscere usando la normale diligenza, la falsità dell'apparente provenienza della firma (par. 64a e 65a); Utah DSA, cit., (sec. 46-3-406) ammette che il titolare del certificato provi (inversione dell'onere della prova) che la firma è stata apposta da altri (o perché è stata sottratta la chiave privata, o perché il certificato è falso); nel contempo, però, il titolare deve provare, nel caso di sottrazione della chiave, che non ha violato i doveri di diligenza nella sua custodia; inoltre, deve sempre provare che il destinatario era a conoscenza della falsità della firma e della violazione dell'obbligo di diligenza.

[75] Ove si ammetta una tale presunzione *juris tantum*, ne deriva che per il disconoscimento della scrittura privata informatica, l'onere della prova risulterebbe invertito rispetto alla scrittura privata cartacea. In quest'ultima, chi risulta sottoscrittore può comodamente dichiarare di non riconoscere la sottoscrizione ed in tal caso grava sulla controparte l'onere di chiedere la verificazione; al contrario, nella scrittura informatica, l'onere di provare la falsità della firma (perché apposta da altri) sarebbe a carico del soggetto che risulta quale sottoscrittore dal relativo certificato. Vedi R. ZAGAMI, ***Firme « digitali »*, 1996, cit., p. 162.**

[76] F. CARNELUTTI, ***Teoria del falso*, Padova, 1935, p. 47.**

[77] La dottrina ritiene che l'assunzione di un nome falso non impedisca il sorgere

Infine, se la falsità riguarda una scrittura privata informatica autenticata *ex* art. 16, in applicazione degli art. 2702 e 2703 c.c. (richiamati dagli artt. 5^1 e 16^1), dovrebbe essere proponibile il rimedio della *querela di falso* ai sensi degli artt. 221 ss. c.p.c.[78].

12. Duplicazione, copie ed estratti del documento.

Riconoscendo il non senso della distinzione tra *originale* e *copia* di un documento informatico, si accoglie pienamente la concezione del documento immateriale, formato dal solo elemento spirituale (contenuto), liberamente trasferibile da un elemento materiale (supporto o contenente) ad un altro, mantenendo la sua originaria efficacia probatoria, e così si afferma che « i duplicati, le copie, gli estratti[79] del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del presente regolamento » (art. 6^1).

Ogni duplicato (o *copia*) di un documento informatico, anche se trasmesso *telematicamente*, possiede la stessa efficacia probatoria dell'« originale », senza che occorra l'intervento di un notaio o altro pubblico ufficiale a garanzia dell'integrità del contenuto. Pertanto, il duplicato di documento non sottoscritto con firma digitale ha l'efficacia probatoria di riproduzione meccanica ai sensi dell'art. 2712 c.c. (art. 5^2); il duplicato di documento sottoscritto con firma digitale ha l'efficacia di scrittura privata ai sensi dell'art. 2702 c.c. (art. 5^1); il duplicato di documento autenticato *ex* art. 16 ha il valore della scrittura privata autenticata *ex* art.

del vincolo contrattuale in capo al contraente falsamente denominatosi. La parte può, infatti, essere comunque esattamente identificata nella sua identità fisica o professionale. La parte identificatasi correttamente potrebbe comunque far valere in certi casi (essenzialità) l'errore sull'identità dell'altro contraente e chiedere l'annullamento del contratto. Vedi M. Bianca, ***Il contratto***, **Milano, 1987, p. 61 ss.**

[78] Si possono immaginare le seguenti ipotesi di infedele autentica notarile: *a*) effettuata utilizzando abusivamente la chiave privata di un notaio; *b*) relativa a firma applicata con una chiave scaduta, revocata o sospesa con regolare pubblicazione (è dovere del notaio controllare la validità attuale della chiave utilizzata, consultando gli appositi registri telematici, art. 16^2); *c*) relativa a firma applicata con una chiave non revocata o sospesa, ma utilizzata da persona diversa del legittimo titolare (il notaio dovrà accertare la corrispondenza tra identità del firmatario e generalità del titolare della chiave che risultano dal certificato, art. 16^2). Ammettendo la querela di falso, nell'ultima ipotesi, colui che appare falsamente come firmatario, otterrebbe una certa tutela, anche in mancanza di revoca della chiave; a differenza di quanto accade, invece, per la semplice scrittura privata informatica non autenticata, per la quale, come si è visto, la revoca non pubblicata non è opponibile. Nelle ultime due ipotesi suddette, la tutela della parte è ulteriormente rafforzata dalla responsabilità civile a carico del notaio (art. 76 l. not.).

[79] « La copia è la riproduzione integrale dell'atto; l'estratto è la riproduzione integrale di una o più parti dell'atto; il certificato è un sunto del contenuto dell'atto », M. Di Fabio, ***Manuale di notariato***, **cit., p. 195.**

2703 c.c.; il duplicato della copia informatica (*ex* art. 6^2) di un atto pubblico cartaceo ha il valore di atto pubblico *ex* art. 2700 c.c.

L'intervento del pubblico ufficiale è, invece, indispensabile per conservare l'efficacia probatoria del documento, quale garanzia dell'integrità del contenuto, nel passaggio dal contenente carta (o altro non informatico) al contenente informatico, in modo analogo a quanto accade per le copie fotografiche di scritture (art. 2719 c.c.)[80]. In tal senso, si prevede la figura *delle copie informatiche autenticate di documenti cartacei* (o, comunque, non informatici), le quali « sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato » (art. 6^3, art. 16^4)[81].

Applicazione del suddetto principio è l'art. 6^2, il quale attribuisce l'efficacia probatoria della scrittura privata o dell'atto pubblico originale, alle copie informatiche spedite o rilasciate ai sensi degli artt. 2714 e 2715 c.c., se ad esse è apposta o associata la firma digitale del pubblico ufficiale che le rilascia (art. 6^2). La norma, pur non riferendosi espressamente alle copie informatiche di originali *cartacei*, richiedendo l'apposizione della firma digitale del pubblico ufficiale, implicitamente si riferisce a questa ipotesi, in quanto, come già detto, la firma del pubblico ufficiale *ex* art. 6^2 non dovrebbe essere richiesta per il rilascio di copie di scritture private che il notaio ha in deposito già in forma informatica con firma digitale. Le copie rilasciate *ex* art. 6^2 possono essere prodotte ed esibite in luogo dell'originale cartaceo (art. 6^4) ed, inoltre, potranno poi essere ulteriormente duplicate senza necessità di un altro intervento notarile[82].

---

[80] Vedi R. ZAGAMI, ***Firme « digitali »*, 1996, cit., p. 152, in particolare nota n. 5.**

[81] L'autentica da parte del pubblico ufficiale dovrà consistere in una « dichiarazione allegata al documento informatico e asseverata con le modalità indicate dal decreto di cui al comma 1 dell'articolo 3 » (art. 6^3); inoltre, è evidentemente indispensabile, l'apposizione della firma digitale del pubblico ufficiale, così come è previsto per la particolare e più specifica ipotesi del comma 2. L'intervento di un notaio o altro pubblico ufficiale ai sensi dell'art. 6^3, dovrebbe attualmente essere richiesto anche per la duplicazione e trasmissione telematica dei documenti informatici (sprovvisti di firma digitale) memorizzati in CD-WORM (*Compact Disk - Write Once Read Many*), volendo mantenere la loro efficacia probatoria originaria, inscindibilmente legata al tipo di supporto utilizzato (fisicamente non riscrivibile e quindi indelebile ed inalterabile), basata sul *legame fisico tra contenuto e contenente*, così come è per i documenti cartacei. Vedi art. 2^{15} l. 537/1993, Deliberazione dell'AIPA 28-7-1994 n. 15, quest'ultima in corso di revisione con l'introduzione dell'uso della firma digitale per garantire l'autenticità in caso di duplicazione o trasmissione telematica. Vedi R. ZAGAMI, ***Firme « digitali »*, 1996, cit., p. 165 s. e ID., *Profili giuridici della firma digitale*, in *Rapporto TI* 1996 dell'FTI, Milano, 1996, p. 248 s.**

[82] L'intervento del notaio che appone la sua firma, a garanzia dell'integrità nella fase di duplicazione, dovrebbe essere richiesto anche nel caso di rilascio di copie informatiche di documenti già depositati presso di lui in forma informatica, ma

Non è disciplinato il passaggio inverso, dal supporto informatico al supporto non informatico (carta o altro), cioè l'effettuazione di *copie cartacee di documenti informatici* (con o senza firma digitale). Anche in questa ipotesi, affinché alla copia cartacea sia attribuito il valore probatorio dell'originale informatico, è indispensabile l'intervento del notaio o del pubblico ufficiale che attesti la conformità della copia su carta (in applicazione estensiva dell'art. 2719 c.c.).

13. Trasmissione del documento.

Mentre la prova della creazione di un documento informatico, riguardo alla provenienza da un certo soggetto, alla sua integrità ed al momento della sua creazione, può essere facilmente ottenuta combinando la verifica di una firma digitale certificata e di una validazione temporale (cosiddetto *non ripudio da parte dell'origine)*, più problematico è fornire la prova dell'avvenuta ricezione di un documento spedito telematicamente per posta elettronica (*non ripudio da parte del destinatario)*. E' evidente che, quando dalla ricezione di un atto possono derivare conseguenze sfavorevoli, il destinatario non avrà alcun interesse a restituire al mittente una ricevuta di ritorno per posta elettronica.

L'art. 12 prevede un'*elezione di domicilio informatico* (o di più domicili speciali *ex* art. 47 c.c.), stabilendo che « il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato ».[83] La nozione di indirizzo elettronico, è fissata quale « identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici » (art. 1 lett. *j*), come ad es. la casella di posta elettronica (*electronic mailbox*) nella rete Internet.

La norma non parla espressamente di presunzione, né ammette (ma nemmeno esclude) la prova contraria circa il fatto della mancata o incorretta ricezione, quali eventi non improbabili, che possono essere determinati da un malfunzionamento dell'*hardware* o del *software* preposti alla trasmissione, gestione e conservazione della messaggistica elettronica[84]. Pertanto, si dovrebbe ritenere

non aventi il valore di scrittura privata o atto pubblico perché sprovvisti di firma digitale.

[83] La dichiarazione dell'indirizzo ai sensi dell'art. 1 lett. *j*, sarebbe opportuno renderla obbligatoria, contestualmente alla richiesta di certificazione, e risultante dai certificati stessi.

[84] Questo è tanto più vero per il più diffuso sistema di posta elettronica in un *open network*, quello nella rete Internet, congenitamente insicuro, dato che i messaggi compiono tortuosi percorsi attraversando molteplici elaboratori di diversa appartenenza, prima di giungere dal computer del mittente a quello del destinatario finale.

che l'art. 12 ponga solo una presunzione *juris tantum* di ricezione che ammette una prova contraria da parte del destinatario incolpevole, come è d'altra parte previsto dall'art. 1335 c.c., da ritenersi applicabile per analogia (insieme al collegato art. 1334 c.c.) anche al caso della trasmissione telematica.

Dalla formulazione letterale dell'art. 12 sembra che il mittente debba solo dare prova dell'avvenuta *trasmissione* (principio della spedizione)[85] perché si verifichi la presunzione di *ricezione* a carico del destinatario. Tale prova, in caso di contestazione, è tutt'altro che facile, dato che si basa su dati informatici facilmente modificabili quali sono le memorie degli elaboratori preposti ai servizi di posta elettronica. Pertanto, il mittente che intenda precostituirsi la prova della trasmissione, avrà *l'onere* di rivolgersi anche in questa situazione ad un terzo garante, agente come una sorta di ufficiale giudiziario, con il compito di filtrare i messaggi e di certificare la loro avvenuta spedizione e ricezione[86], anche con riferimento ai profili temporali (art. 12^2).

È detto, poi, che « la trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge » (art. 12^3). Si fa qui implicito riferimento, oltre che alle norme del c.p.c., anche alla l. 890/1982 ed alla l. 53/1994 che consentono la notificazione a mezzo del servizio postale, senza però l'intervento dell'ufficiale giudiziario, che andrebbe sostituito dal terzo garante con le modalità che verranno stabilite[87].

---

[85] Il *principio della spedizione* (efficacia della volontà non appena trasmessa all'altra parte), si contrappone al *principio della cognizione* (efficacia della volontà nel momento in cui sia conosciuta dall'altra parte) codificato nell'art. 1326 c.c., con il temperamento della presunzione di cui all'art. 1335 c.c. (*principio della ricezione*).

[86] Così anche la *Relazione* al regolamento, per la quale « si tratta [...] del passaggio *obbligato* del documento attraverso un sistema informatico, programmato secondo criteri che garantiscono l'apposizione di una data e di un orario certi e verificabili ».

[87] La disposizione dell'art. 11^1, la quale stabilisce che « i contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma digitale secondo le disposizioni del presente regolamento sono validi e rilevanti a tutti gli effetti di legge », non è strettamente necessaria, dato che la validità e rilevanza di tali contratti già deriva, comunque, dall'affermata validità e rilevanza del documento informatico. Lo stesso per la disposizione che rinvia al d.lgs. n. 50/1992, disciplinante le cosiddette vendite telematiche (art. 11^2), in quanto l'art. 9 dello stesso provvedimento ne stabilisce espressamente l'applicabilità anche « ai contratti conclusi mediante l'uso di strumenti informatici e telematici ». Piuttosto, poiché non si affrontano i problemi del luogo e del momento di conclusione del contratto nelle reti telematiche, si applicheranno, le norme ordinarie in tema di conclusione del contratto tra assenti (artt. 1326 ss. c.c.), riferendole però ad atti preparatori (proposta ed accettazione) in forma informatica, ed all'indirizzo elettronico di cui agli artt. 1 lett. *j* e 12. Sulla conclusione del contratto nelle reti telematiche vedi G. FINOCCHIARO, ***I contratti informatici***, Padova, 1997.